

Il faut sauver le soldat Alexander !

Très officiellement auditionné le 15 octobre par les sénateurs Mark Udall et Patrick Leahy de la commission du renseignement du Congrès, le général Keith Alexander, chef de la NSA, a reconnu que « seuls un ou deux complots terroristes avaient été réellement déjoués » grâce aux interceptions effectuées par son administration.

On peut tout de même s'étonner que le général Alexander ne se montre pas plus précis ou que la mémoire lui fasse à ce point défaut. Compte tenu du budget d'environ 15 milliards de dollars alloué à la NSA (25 fois le budget total de la DGSE), il serait important de savoir si c'est un ou deux complots terroristes qui ont été déjoués. En tant qu'ancien responsable d'un service de sécurité j'aurais eu à cœur, en ce qui me concerne, de démontrer ainsi le doublement du rendement de l'administration dont j'avais la charge. L'imprécision est d'autant plus surprenante que, quand il s'agissait il y a quelques mois de justifier la chasse donnée à l'indélicat Edward Snowden, le général Alexander avait péremptoirement assuré avec toute la rigueur mathématique du diplômé en sciences de West Point qu'il est, que pas moins de 54 « *complots ou actions terroristes* » avaient été repérés et déjoués « *dans plus de 20 pays à travers le monde* » grâce aux interceptions de la NSA. Les sénateurs de la commission d'enquête ont eu le tact de ne pas mettre le chef de la NSA en difficulté en lui demandant ce qu'il en était des 52 ou 53 attentats manquants et des 20 pays (au moins) épargnés. Le sénateur Udall s'est contenté de conclure que « *La preuve ne nous a jamais été apportée que la collecte indifférenciée de données a fourni des renseignements de valeur ayant conduit individuellement à déjouer des attentats* ».

On observera qu'à l'exception du journal « Le Monde » dans sa version électronique du 16 octobre, pratiquement aucun média français n'a cru devoir faire état de cet incident pourtant significatif à bien des égards. Baignée d'évangélisme, la culture américaine tient le mensonge pour une abomination et l'a même érigé au rang de crime sur le plan pénal. Mais comme, en définitive, on ne ment pas moins aux Etats-Unis qu'ailleurs, il a bien fallu trouver un moyen de dissimuler le mensonge sous des apparences respectables et le seul moyen de parvenir à cette fin est de l'habiller du voile protecteur du secret et si possible de la forme la plus inviolable du secret qu'est le secret de défense. C'est ainsi que la technostructure US a développé le système protocolaire de classification et de protection du secret parmi les plus contraignants du monde qui va jusqu'à interdire à des gens travaillant sur le même dossier d'en parler entre eux et avait suscité dans les années 60 la fameuse boutade : « *My job is so secret that I'm not allowed to know what I am doing* ».

Les choses n'ont pas changé depuis et se sont même aggravées. Les 16 agences de renseignement américaines et leurs quelque 300000 fonctionnaires ne communiquent entre elles

que contraintes et forcées, et avec beaucoup de mauvaise grâce, par la seule autorité du Président et « commandant en chef » qui s'épuise vite à ce petit jeu et ne peut résoudre chaque cas litigieux, tous les cas étant a priori litigieux. Quant à communiquer avec des services étrangers, fussent-ils amis et alliés, cela relève au mieux de l'égarement psychiatrique et au pire de la haute trahison. Les services alliés sont priés de répondre aux questions posées, dans les formes et les délais prescrits par le service US demandeur, sans avoir à en connaître les tenants et aboutissants. Solliciter la connaissance de la suite donnée aux informations fournies relève d'une incongruité vite signalée aux autorités politiques de l'impertinent avec demande de sanctions à la clef.

C'est dans ce contexte, et largement stimulées par les suites du 11 septembre et les dispositions du Patriot Act, que se sont développées la culture et la logique d'entreprise des agences de renseignement américaines et en particulier celle de la NSA dont le rôle a de plus été magnifié par l'explosion des communications électroniques relevant de sa compétence au cours des vingt dernières années. Depuis sa création en 1952, la NSA est tout à fait officiellement chargée à l'échelle planétaire du recueil par moyens techniques du renseignement circulant par voie hertzienne ou filaire et susceptible de concerner la sécurité ou les intérêts des États-Unis. Vaste programme, car compte tenu de la puissance du pays et de sa vocation mondiale, du rôle de réserve de sa monnaie et de ses alliances économiques et militaires, tout et n'importe quoi est susceptible d'être considéré comme interférant avec sa sécurité et ses intérêts. On ne saurait reprocher à la NSA d'essayer de s'acquitter de la mission qui lui a été réglementairement confiée. Et elle le fait avec d'autant plus d'ardeur et de façon d'autant plus extensive, qu'elle est soumise, comme tout le monde outre-atlantique, à la dictature du « publish or perish » et à de drastiques impératifs de rendement quantitatif - la quantité étant toujours plus incontestablement et immédiatement mesurable que la qualité, comme l'ont très bien compris en France les virtuoses de la RGPP.

Il n'y a donc pas lieu d'être surpris que la NSA, qui dispose pour ses missions de moyens humains et financiers considérables¹, se soit livrée sans retenue et de la manière la plus extensive possible aux tâches qui lui étaient assignées. On peut lui reprocher, comme l'a fait la commission ad hoc du Sénat, d'avoir un peu exagéré ses résultats, mais certainement pas de les avoir obtenus par des moyens qui violent la légalité ou les usages internes et internationaux. La NSA n'est pas un service secret. Tout le monde sait qu'elle existe et connaît son adresse. Son chef est nommé par le Président avec l'accord du Congrès, son budget est publié et elle entretient un site Internet. Mais la NSA est un service spécial. Si tous les États du monde, y compris les grandes démocraties, entretiennent souvent à grands frais des services spéciaux, ce n'est pas pour faire

¹ La NSA dispose d'un budget annuel estimé à 15 milliards de dollars et compte environ 38000 fonctionnaires assistés de plus de 15000 sous-traitants (dont Edward Snowden...). Pour être à parité et rapporté à la population respective, la direction technique de la DGSE qui remplit en France les mêmes missions devrait disposer de 10000 agents (elle en compte 2000) et d'un budget de 2 milliards d'euros (elle dispose de 300 millions d'euros).

double emploi avec les différentes administrations chargées de la collecte et du traitement des informations légalement acquises. C'est pour s'affranchir, quand le politique le juge nécessaire et sans en prendre la responsabilité, de la légalité interne et internationale, de ses engagements officiels et du respect de la parole donnée.

C'est bien pourquoi il est dérisoire et risible de vouloir proposer à l'exécutif américain de signer une « code de bonne conduite » l'engageant à respecter ce qu'il était de toute façon supposé respecter et qu'il a délibérément fait violer en toute connaissance de cause par ses services mandatés à cet effet. Il ne fait aucun doute que le Président américain, sauf à avoir perdu tout sens de l'humour, signera des deux mains un tel engagement, sachant que sous couvert du secret ses services spéciaux continueront à poursuivre leur mission qui est précisément de l'affranchir de ce genre de contrainte. Et au-delà du ridicule, une telle demande est même dangereuse car que feront les demandeurs de code de bonne conduite si il apparaît que le dit code n'est pas respecté ? Quand on n'a pas les moyens de ses exigences, il est préférable de ne pas en formuler.

La machine sécuritaire américaine est incontestablement devenu folle. L'inepte « guerre globale à la terreur » en est en grande partie responsable. Au lendemain du crime du 11 septembre, il convenait de faire la guerre à des criminels terroristes, donc à un groupe restreint, à ses idéologues, à ses sponsors, à ses financiers. Autant de cibles identifiables et vulnérables. Au lieu de quoi l'Amérique s'est lancée dans une guerre à un concept qui n'est ni quantifiable ni localisable, ce qui ne pouvait que conduire ses services de renseignement à placer la planète entière, y compris ses propres citoyens, sous une loi permanente des suspects à surveiller de près. Si les résultats pratiques de la démarche en matière d'antiterrorisme n'ont pas été à la hauteur, comme en est convenu piteusement le chef de la NSA, les bénéfices collatéraux de la manœuvre sont incommensurables puisqu'ils ont permis à l'administration américaine de développer en toute bonne conscience et avec un imparable alibi moral, un système planétaire d'acquisition de renseignement politique, diplomatique, économique et industriel sans même avoir à se livrer au jeu toujours dangereux et coûteux de recrutement de sources humaines.

Dans les années 70, il avait fallu à la Stasi recruter et rémunérer un tiers de la population de la RDA pour connaître 20% de « la vie des autres ». Aujourd'hui, il suffit à la NSA de s'abonner aux réseaux sociaux pour connaître sans se fatiguer 80% de leur vie privée que les milliards de gentils internautes étalent complaisamment sur le net. Car, contrairement au renseignement humain ou opérationnel, le renseignement technique ne permet de connaître que ce que ses cibles veulent bien étaler via les courants électriques et les ondes électromagnétiques. C'est bien la complaisance des cibles qui fait la fortune de la NSA et de ses semblables dans le monde. Au siècle dernier, pour violer la correspondance privée, il fallait en ouvrir l'enveloppe à l'insu du destinataire, ce qui était considéré un peu partout comme un crime ou un délit. Mais quand on confie sa correspondance à un flux d'ondes qui se promènent dans l'atmosphère ou le long de

filis au trajet indéterminé, on ne peut s'étonner que, malveillance ou pas, elle finisse par atterrir n'importe où. Au milieu de la décennie écoulée, nos responsables politiques et économiques exhibaient fièrement leurs Blackberrys tout neufs dans les salons branchés, les réunions « exécutives » et les séminaires « corporates ». Jusqu'à ce qu'on s'aperçoive que tout le réseau Blackberry était sous contrôle de la NSA. Toute la bien-pensance parisienne s'est indignée pendant quinze jours de cette effroyable entorse aux règles de « bonne conduite ». Et tout ce petit monde d'oublier très vite l'incident et de troquer son Blackberry déjà has-been contre le dernier smartphone à la mode... directement branché sur les serveurs de Cupertino, Californie....

Car non contents d'échanger leurs informations sur des réseaux manifestement sous surveillance, nos politiques et nos chefs d'entreprises vont même maintenant jusqu'à stocker les informations qu'ils n'échangent pas directement sous les yeux attentifs et intéressés de la NSA. Le fameux « cloud » auquel les marchands américains de matériels et de logiciels informatiques nous incitent vivement, voire nous obligent, à confier toutes nos données personnelles et professionnelles n'est pas un lieu éthéré confié à la garde d'ectoplasmiques séraphins. Il s'agit de serveurs informatiques situés à 95% sur le sol américain et auxquels la NSA a le plus réglementairement du monde accès. En gros, ce type de fonctionnement revient à enfermer sa fortune dans un coffre, à confier le coffre à des voleurs et à leur donner les clés du coffre en leur demandant bien sûr un engagement écrit de ne pas s'en servir...

Alors, avant de se laisser aller à des mouvements d'indignation sans lendemain et en attendant d'avoir les moyens politiques de leur indignation, les dirigeants politiques et économiques européens feraient peut être mieux d'essayer de comprendre pourquoi nos systèmes de communications et de traitement des données sont à ce point transparents pour l'ami américain et d'en tirer les conséquences aussi bien sur le plan de leur comportement individuel que sur les mesures collectives à prendre dans ce domaine pour préserver notre liberté et notre dignité.